CS 4371.001
Group 27 - Security Project 1

Leonardo Bujanda Carmona

Alexander Martin

Taslima Keya

Kristopher Hinkel

Project Due Date: 10/5/2021

Section I

Summarize what you have done in the project and clearly state the responsibility of each group member, e.g. who did which task, who wrote which part of the report, how your group was coordinated, etc.

Responsibilities:

- Leonardo Bujanda
  - Task: II, IV, V
  - Report: Section I, II, IV, V

- Alexander Martin
  - Task: Task III
  - Report: Section: III, V

- Kristopher Hinkel
  - Task: -
  - Report: -

- Taslima Keya
  - Task: Task III
  - Report: Task III

Group Coordination:

Our group communicated primarily using Discord. We discussed and partitioned the labor throughout all of us, and communicated any thoughts and concerns that we might have had. Any issues, troubles, or questions were discussed in our Sunday afternoon meetings.

Section II

a) Show the NMap commands to scan the computers and the service ports.

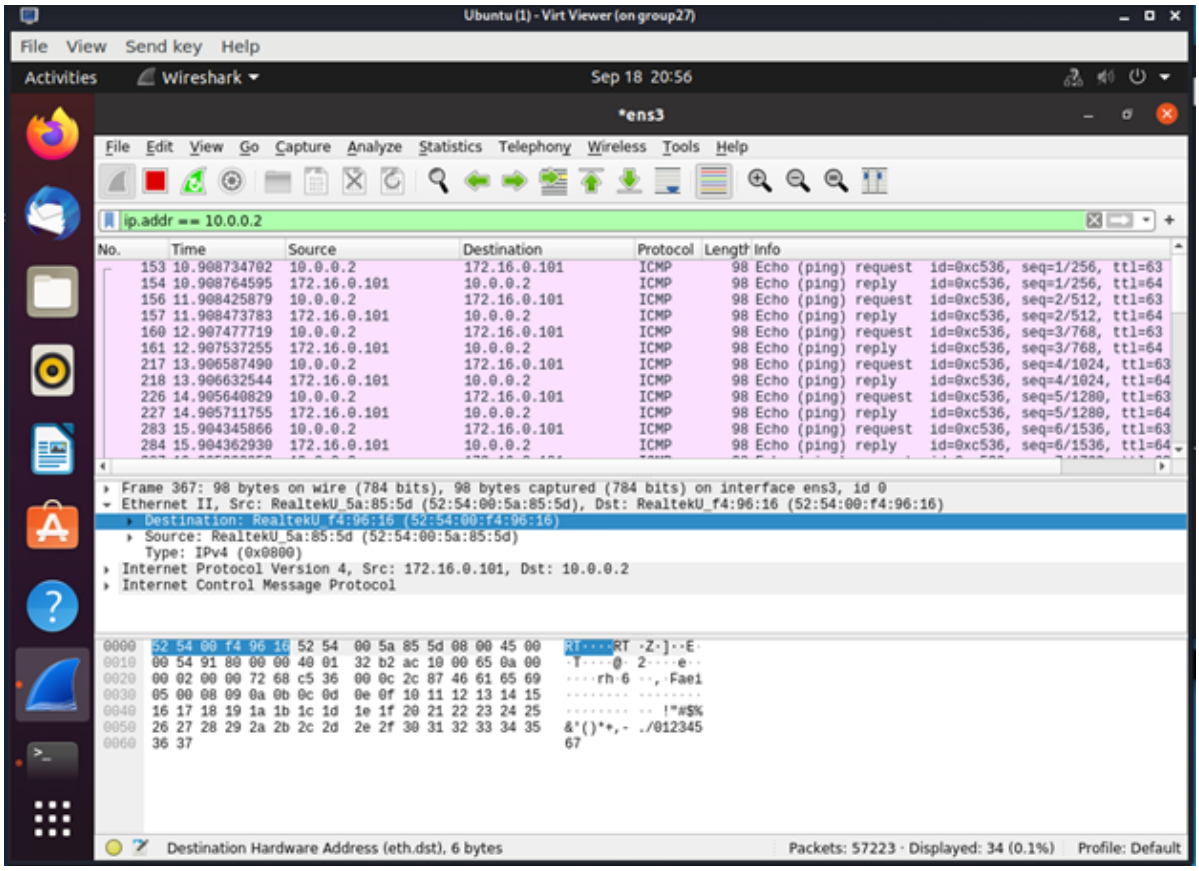
```
root@kali:~# nmap 172.16.0.000/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-10 05:09 EDT
Nmap scan report for 172.16.0.1
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 52:54:00:F4:96:16 (QEMU virtual NIC)

Nmap scan report for 172.16.0.101
Host is up (0.000076s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 52:54:00:5A:85:5D (QEMU virtual NIC)

Nmap scan report for 172.16.0.102
Host is up (0.0000030s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 27.71 seconds
```

b) Show the discovered IPs and services in Network A and B (screenshots).

```
root@kali:~# nmap 10.0.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-10 05:21 EDT
Nmap scan report for 10.0.0.1
Host is up (0.00090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.0.2
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 10.0.0.3
Host is up (0.0016s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/tcp open  rpcbind

Nmap done: 256 IP addresses (3 hosts up) scanned in 49.19 seconds
root@kali:~#
```

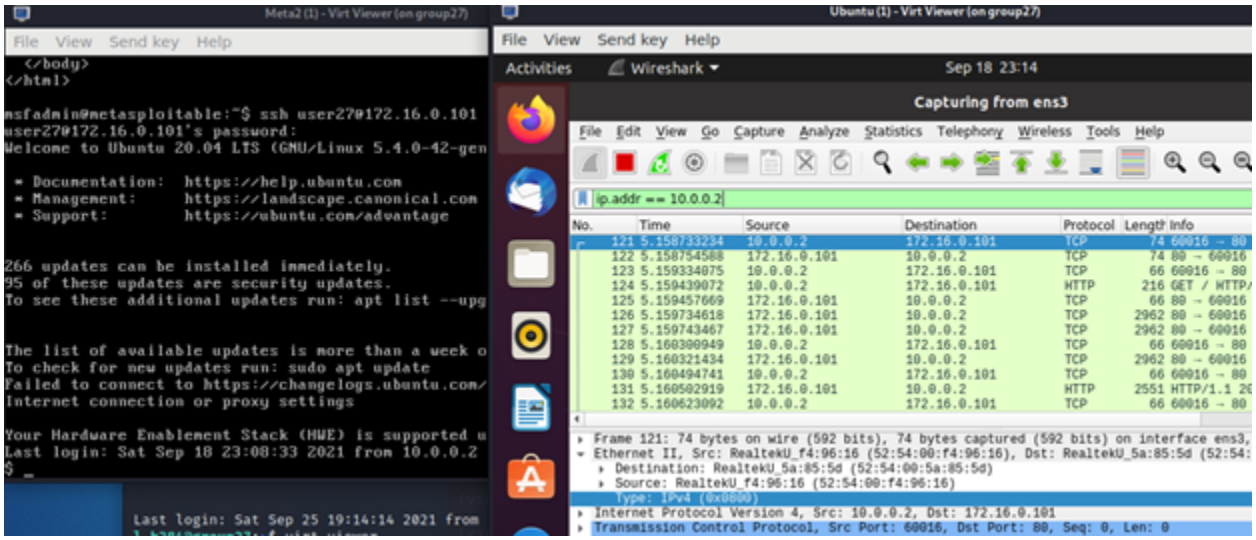
c) Show the Wireshark results (screen shots) of checking the web service between B.1 and A.1, and between A.2 and A.1. State if web service is allowed between computers.

(Ping between B.1 and A.1)



Ping is ALLOWED between from B.1 to A.1

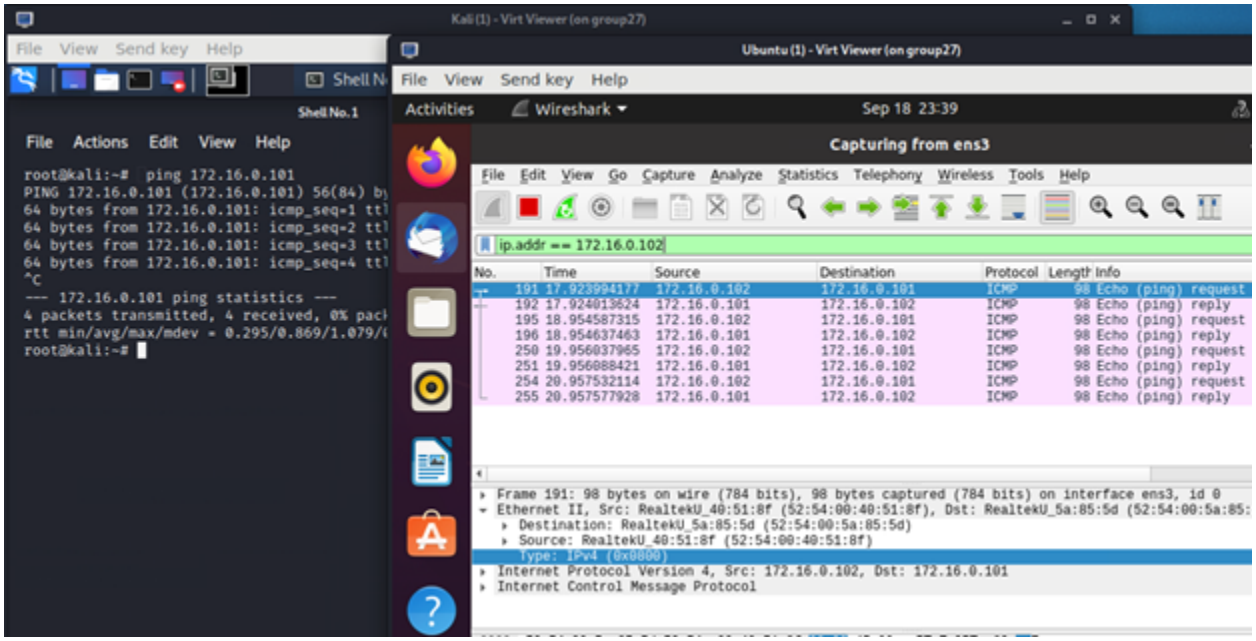
(Web Service Between B.1 and A.1)



Web service IS allowed between the computers, curl and SSH is fully function from B.1 to A.1

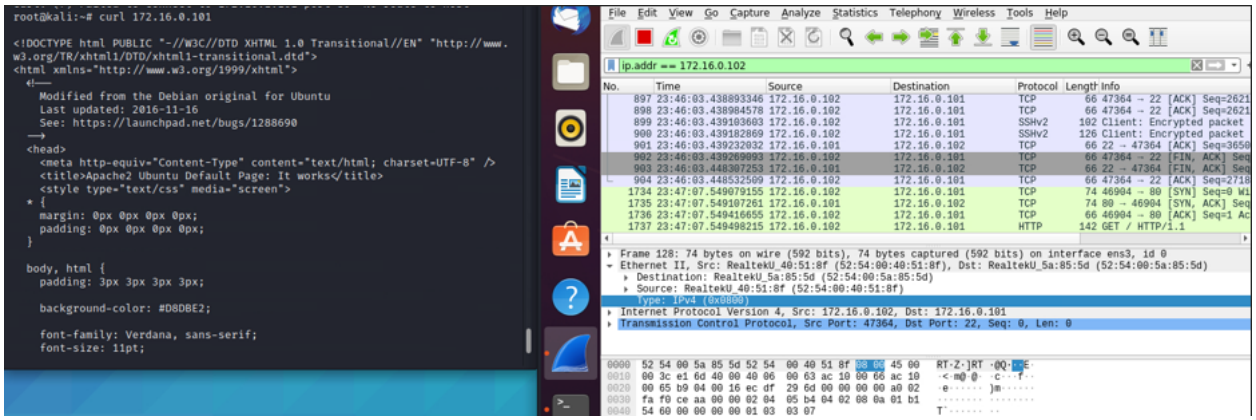
d) Show the Wireshark results (screen shots) of checking the ping between between B.1 and A.1,and between A.2 and A.1. State if ping is allowed between computers.

(Ping between A.2 and A.1)



Ping IS allowed between the computers. As shown above, I can ping 172.16.0.101(A.1) from 172.16.0.102(A.2).

(Web Service between A.2 and A.1)



Web service is allowed between A.2 and A.1. Curl and SSH both fully function from A.2 to A.1.

Section III

a) Show the access control matrix.

	Server	Workstations	Ex Computers
Server	NA	icmp	icmp
Workstations	ssh 443 icmp 80	NA	icmp 443 80
External Computers	443 80	NA	NA

b) Find and explain which policy CANNOT be completely enforced by the iptables of R.

a) The server provides only web service to external computers.
b) The server provides only SSH and web service to the workstations.

- The iptables are set for R so once packets have passed through the router, the network doesn't filter the packets within the network allowing possible exploitations. A.1 (the server) cannot be configured in this specific way directly from iptables of R, must be from within A.1. The iptables of R only moderate traffic from Network A and any outer Network, A.1 must's services must be changed from the actual A.1.

c) The server shall not access any services of any external computers.
d) The workstations shall not provide any services.

- This is a rule that is specific to the inside of Network A. Configuring the iptables of R can only affect what comes out and into Network A, not what happens inside of it. Workstations themselves must be modified to enforce this, as the traffic of the inside of Network A cannot be fully moderated by R.

e) The workstations can access the services hosted by the server.
f) The workstations can access only the web service provided by external computers.
g) The workstations and the server can ping to any other computers
h) External computers cannot ping to the workstations or the server.

c) Show the iptables rules (iptables -S) in R. Explain the purpose of each iptables rule.

```
$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-N ICMP
-N TCP
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -s 172.16.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.0.0/24 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -j DROP
-A FORWARD -s 172.16.0.0/24 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -p tcp -m tcp --sport 80 -j ACCEPT
-A FORWARD -j DROP
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -j DROP
$
```

-INPUT -p tcp -m tcp --dport 80 -j ACCEPT

- *Accept inputs into port 80*

-INPUT -s 172.16.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT

- *Only ips from the specified network 172.16.0.0/24 can access ssh*

-INPUT -s 172.16.0.0/24 -p icmp -m icmp --icmp-type 8 -j ACCEPT

- *Only ips from the specified network 172.16.0.0/24 can access ping*

-INPUT -j drop

- *Drop everything else*

-FORWARD -s 172.16.0.0/24 -p icmp -m icmp --icmp-type 8 -j ACCEPT

- *Only allow pings from the network 172.16.0.0/24 to be forwarded*

-FORWARD -p tcp -m tcp --dport 80 -j ACCEPT

- *Allow web services to be forwarded*

-FORWARD -p tcp -m tcp --sport 80 -j ACCEPT

- *Allow web services to be forwarded*

-FORWARD -j DROP

- *Drop anything else*

OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

- *Any established or related connections may be allowed to be outputted*

OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

- *Allow web services to be outputted*

OUTPUT -j DROP

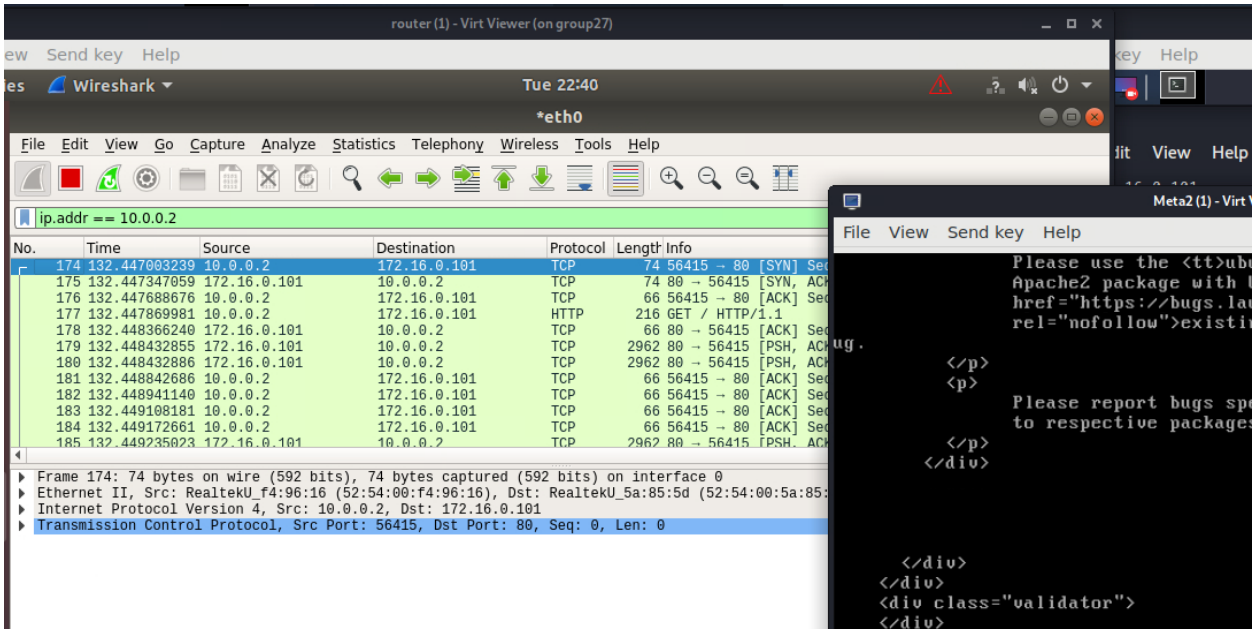
- *Drop everything else*

Section IV

a) Show the NMap results (screenshots) of the exposed computers and ports of Network A.

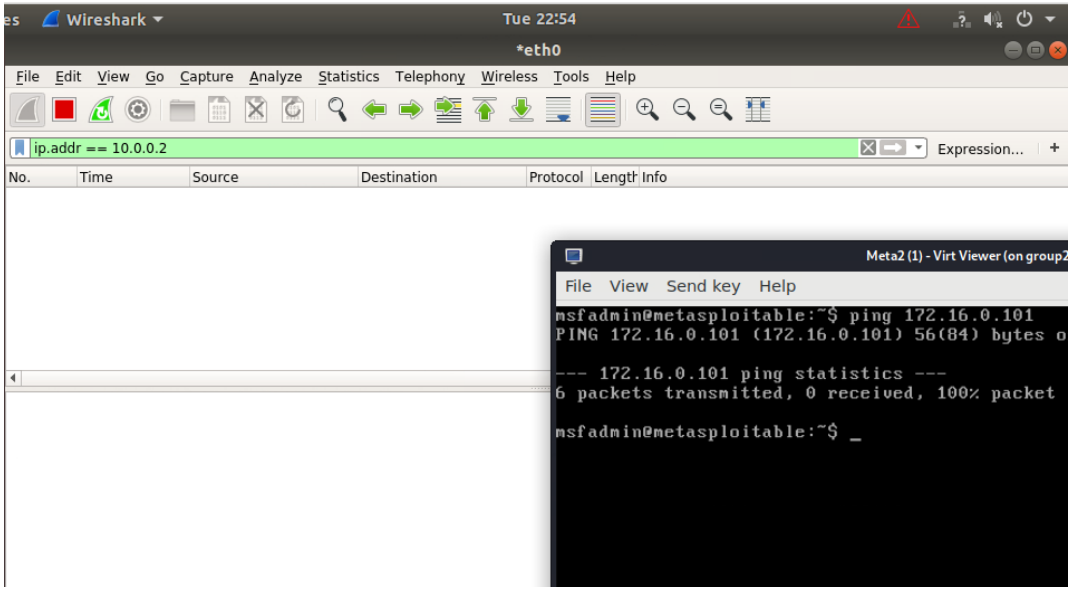
```
msfadmin@metasploitable:~$ nmap 172.16.0.0/24

Starting Nmap 4.53 ( http://insecure.org ) at 2021-09-28 23:28 EDT
Interesting ports on 172.16.0.1:
Not shown: 1713 filtered ports
PORT   STATE  SERVICE
80/tcp closed http

Interesting ports on 172.16.0.101:
Not shown: 1713 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Interesting ports on 172.16.0.102:
Not shown: 1713 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 34.817 seconds
msfadmin@metasploitable:~$
```

b Show the Wireshark results (screenshots) of checking the web service between B.1 and A.1. State if web service is allowed between computers.



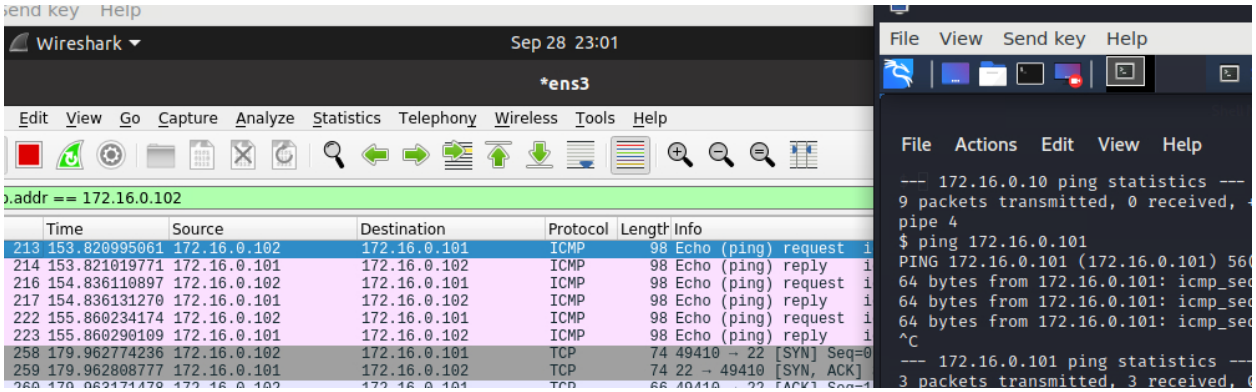
Web Service IS ALLOWED between b.1 and a.1, but ssh is clearly not allowed and blocked by iptables rules.

c) Show the Wireshark results (screenshots) of checking the ping between B.1 and A.1. State if ping is allowed between computers.



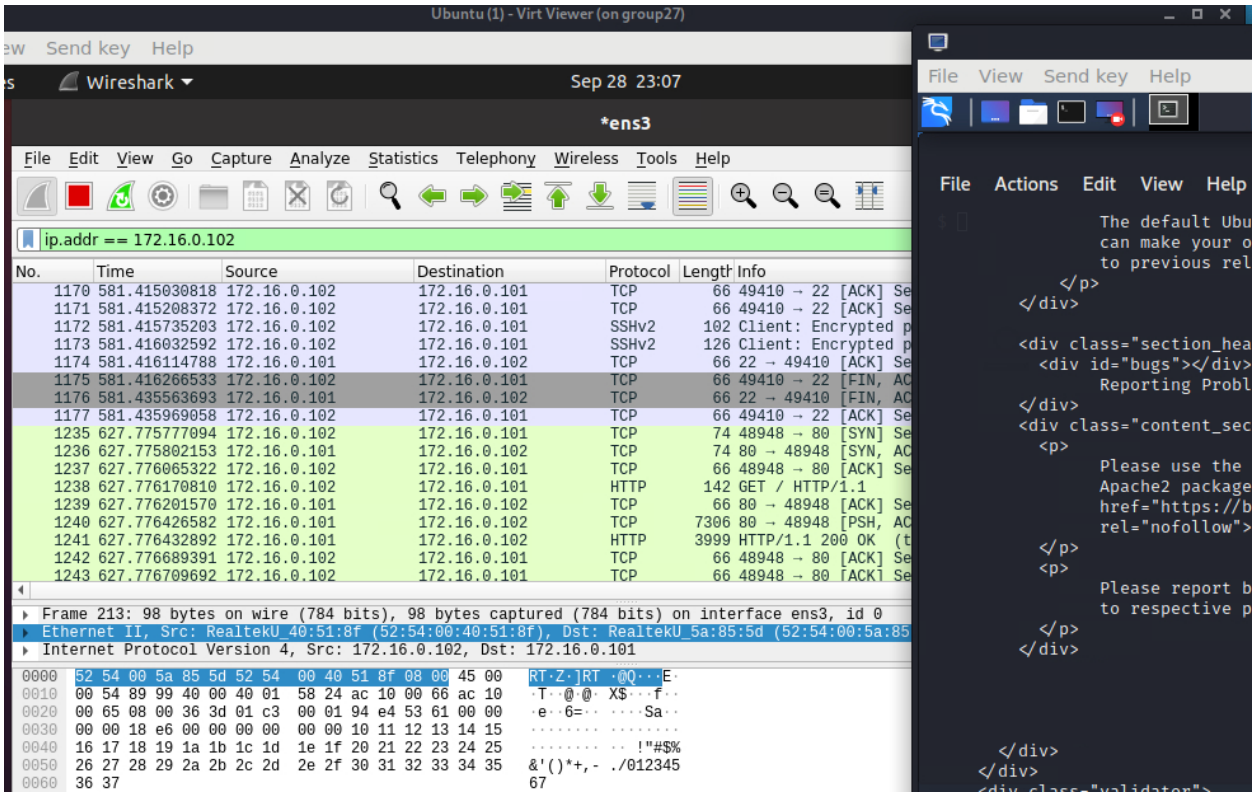
Ping is NOT allowed between b.1 and a.1, nothing shows in the wireshark because the iptables are being enforced.

c) Show the Wireshark results (screen shots) of checking the ping between A.2 and A.1. State if ping is allowed between computers.



Ping is allowed between computers the computers a.2 and a.1.

b Show the Wireshark results (screenshots) of checking the web service between A.2 and A.1. State if web service is allowed between computers.



Web Service is allowed between computers A.2 and A.1, and sshing from A.2 to A.1 is also allowed. Curling from A.2 to A.1 is allowed.

Section V

a) Show the iptables rules (iptables -S) to enforce the security policy in A.1 that is not implemented in R. Explain each iptables rule.

b)The server provides only SSH and web service to the workstations
d)The workstations shall not provide any services
Once packets have passed R we must maintain the security policy of only providing SSH and web service to the workstations only. Prohibiting all external computers from these specific services.

```
sudo iptables -A INPUT tcp --dport 22 -s 172.16.0.0/24 -j ACCEPT
sudo iptables -A INPUT tcp --dport 80 -s 172.16.0.0/24 -j ACCEPT
sudo iptables -A INPUT -j DROP
sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -j DTOP
```

b) Show the iptables rules (iptables -S) to enforce the security policy in A.2 that is not implemented in R. Explain each iptables rule.

b) The server provides only SSH and web service to the workstations.
d) The workstations shall not provide any services.

Because A.2 is a workstation and should not be providing any services, we must now allow any sshing or http into A.2. However, we must still allow ping A.2 to ping to any computer and be pinged from Network A. We can accomplish this with the following rules:

```
sudo iptables -A INPUT -p --icmp-type echo-request -s 172.16.0.0/24
sudo iptables -A INPUT -j DROP

sudo iptables -A -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p --icmp-type echo-reply  -j ACCEPT
sudo iptables -j DROP
```

c) Assume the company only stores classified business data in Computer A.1, and does not allow anyone to carry a device to transfer data. Users have accounts on A.1 to access the data. Discuss whether or not the security policy can ensure that the classified data will not be disclosed to external computers through network. Be as specific as possible in your discussion. For example, if you do not think the security policy is secure, you shall show which item of the policy has problem or what policy is missing.

(I am assuming we are discussing only the policy implemented with R, and now the additional adjustments made in 5.a and 5.b)

Through the policy implemented in R that follows the requirements set by the guidelines, we do not think that the policy would be fully secure. It is true that users from the external network cannot ssh into any computer within Network A thanks to the rules. However, it is true that the external computers only have access to port 80 on Computer A.1.

The security risk lies in the fact that a malicious actor user within Network A that has access to Computer A.1 could provide a web service that leaks the data that Network A is trying to disclose. If leaked data is shown on port 80 of any computer within Network A, then they could see that compromised data. The security of the users data is reliant on the Integrity of those with accounts.

Ideally, Network A's computers would be completely isolated from Network B with absolutely zero ports open to them. This way, the data could not be shared in any way. The policy is missing the closing of port 80. The Confidentiality of the companies data would be completely secure from classified data leaks